Docket No. 247046US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hiroaki SAKAGUCHI GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: INFORMATION PROCESSING APPARATUS AND METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-372521	December 24, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

S03P1456 6500

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００２年１２月２４日
出願番号 Application Number: [ST. 10/C]:	特願２００２－３７２５２１ ［ＪＰ２００２－３７２５２１］
出願人 Applicant(s):	ソニー株式会社

２００３年　８月１９日

特許庁長官
Commissioner,
Japan Patent Office　今井康夫

出証番号　出証特２００３－３０６７５９３

【書類名】　特許願
【整理番号】　0290673106
【提出日】　平成14年12月24日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　坂口　浩章
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　情報処理装置および方法

【特許請求の範囲】

【請求項１】　複数のデータを結合して圧縮する圧縮手段と、

前記複数のデータに関する第１の付随データを生成する第１の生成手段と、

前記圧縮手段により圧縮されたデータを、前記第１の生成手段により生成された前記第１の付随データとともに暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記複数のデータは、複数の実行プログラムである

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記第１の付随データは、前記複数のデータの個数および大きさに関するデータである

ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記圧縮されたデータに関する第２の付随データを生成する第２の生成手段と、

前記暗号化されたデータ、および、前記第２の生成手段により生成された前記第２の付随データを格納する格納手段と

をさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記第２の付随データは、前記圧縮されたデータの大きさに関するデータである

ことを特徴とする請求項４に記載の情報処理装置。

【請求項６】　複数のデータを結合して圧縮する圧縮ステップと、

前記複数のデータに関する付随データを生成する生成ステップと、

前記圧縮ステップの処理により圧縮されたデータを、前記生成ステップの処理により生成された前記付随データとともに暗号化する暗号化ステップと

を含むことを特徴とする情報処理方法。

【請求項７】　暗号化されたデータを復号する復号手段と、

前記復号手段により、複数のデータが結合されて圧縮されたデータ、および、前記複数のデータに関する付随データを復元し、前記複数のデータが結合されて

圧縮されたデータを伸張する伸張手段と

を備えることを特徴とする情報処理装置。

【請求項８】　前記複数のデータは、複数の実行プログラムである

ことを特徴とする請求項７に記載の情報処理装置。

【請求項９】　前記付随データは、前記複数のデータの個数および大きさに関するデータである

ことを特徴とする請求項７に記載の情報処理装置。

【請求項１０】　前記付随データに基づいて、前記複数のデータの所在に関する管理テーブルを作成する作成手段と、

前記複数のデータ、および前記作成手段により作成された前記管理テーブルを記憶する記憶手段と

をさらに備えることを特徴とする請求項７に記載の情報処理装置。

【請求項１１】　暗号化されたデータを復号する復号ステップと、

前記復号ステップの処理により、複数のデータが結合されて圧縮されたデータ、および、前記複数のデータに関する付随データを復元し、前記複数のデータが結合されて圧縮されたデータを伸張する伸張ステップと

を含むことを特徴とする情報処理方法。

【請求項１２】　複数のデータを結合して圧縮する圧縮手段と、

前記複数のデータに関する第１の付随データを生成する第１の生成手段と、

前記圧縮手段により圧縮されたデータを、前記第１の生成手段により生成された前記第１の付随データとともに暗号化する暗号化手段と、

前記圧縮されたデータに関する第２の付随データを生成する第２の生成手段と、

前記暗号化されたデータ、および、前記第２の付随データを格納する格納手段と、

前記格納手段に格納されている前記暗号化されたデータを復号する復号手段と、

前記復号手段により、前記圧縮されたデータ、および、前記第１の付随データを復元し、前記圧縮されたデータを伸張する伸張手段と、

前記伸張手段により伸張された前記複数のデータの中から、所定のデータを選択する選択手段と、

前記選択手段により選択された前記所定のデータの処理を実行する実行手段とを備えることを特徴とする情報処理装置。

【請求項１３】　前記第２の付随データに基づいて、前記複数のデータの所在に関する管理テーブルを作成する作成手段と、

前記伸張手段により伸張された前記複数のデータ、および前記作成手段により作成された前記管理テーブルを記憶する記憶手段と

をさらに備えることを特徴とする請求項１２に記載の情報処理装置。

【請求項１４】　前記実行手段は、前記記憶手段に記憶されている前記管理テーブルに基づいて、前記所定のデータの処理を実行する

ことを特徴とする請求項１３に記載の情報処理装置。

【請求項１５】　前記復号手段による復号処理、および前記伸張手段による伸張処理の開始を指示するとともに、前記復号処理および前記伸張処理の終了を通知する通信手段をさらに備える

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１６】　前記複数のデータは、複数の実行プログラムである

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１７】　前記第１の付随データは、前記複数のデータの個数および大きさに関するデータであり、

前記第２の付随データは、前記圧縮されたデータの大きさに関するデータである

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１８】　複数のデータを結合して圧縮する圧縮ステップと、

前記複数のデータに関する第１の付随データを生成する第１の生成ステップと、

前記圧縮ステップの処理により圧縮されたデータを、前記第１の生成ステップの処理により生成された前記第１の付随データとともに暗号化する暗号化ステップと、

前記圧縮されたデータに関する第２の付随データを生成する第２の生成ステップと、

前記暗号化されたデータ、および、前記第２の付随データを格納する格納ステップと、

前記格納ステップの処理により格納された、前記暗号化されたデータを復号する復号ステップと、

前記復号ステップの処理により、前記圧縮されたデータ、および、前記第１の付随データを復元し、前記圧縮されたデータを伸張する伸張ステップと、

前記伸張ステップの処理により伸張された前記複数のデータの中から、所定のデータを選択する選択ステップと、

前記選択ステップの処理により選択された前記所定のデータの処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法に関し、特に、例えば、複数の実行プログラムを圧縮し、圧縮されたデータを、各プログラムの付随データとともに暗号化するようにした情報処理装置および方法に関する。

【０００２】

【従来の技術】

最近、複数のCPUが混載されたLSI（Large Scale Integrated）が使用されることが多くなってきている。また、ソフトウェアソリューション指向のアーキテクチャを採用し、ソフトウェアを入れ替えることで異なるアプリケーションに対応できるLSIが増えつつある。

【０００３】

このため、複数のCPUが混載されたLSIや異なるアプリケーションに対応できるLSIを採用した製品には、同じアーキテクチャのインストラクションセットで構成された複数の実行プログラムが必要であり、それらを保存しておくフラッシュ

メモリなどの不揮発性の記憶手段として、より大容量のものが必要とされ、製品コストを高くする要因となっている。

【０００４】

そこで、例えば、プログラムを圧縮してROMに格納するとともに、圧縮されたプログラムを伸張するためのマップファイルを他のROMに格納することにより、プログラムの容量を削減するようにしている（特許文献１参照）。

【０００５】

また例えば、プログラムの一部を非圧縮状態とし、残りの一部を圧縮してROMに格納することにより、プログラムの容量を削減するようにしているものもある（特許文献２参照）。

【０００６】

また例えば、プログラムを圧縮するとともに、圧縮されたプログラムのヘッダ部分に復元方式に係わる情報を格納しておくことで、プログラムの容量を削減するようにしているものもある（特許文献３参照）。

【０００７】

さらにまた例えば、圧縮されたプログラムと、そのプログラムを展開するための展開プログラムとを一体的にROMに格納することにより、記憶容量を少なくするようにしているものもある（特許文献４参照）。

【０００８】

【特許文献１】

特開平１０－１３３８８０号公報

【特許文献２】

特開平１１－３１２０８９号公報

【特許文献３】

特開平５－３１３９０４号公報

【特許文献４】

特開平７－２４８９２１号公報

【０００９】

【発明が解決しようとする課題】

このように、プログラムを圧縮することにより記憶容量を削減することができるが、ソフトウェアソリューション指向のアーキテクチャにおいては、重要な技術がソフトウェアとして実現されることが多いために、ハードウェアとして実現された技術よりも流用しやすく、単にプログラムを圧縮するだけでは、他社によるリバースエンジニアリングが容易になってしまう恐れがあった。

【００１０】

そこで、重要な技術を守るため、リバースエンジニアリングが困難であるようなプログラム保存方法がいくつか提案されている。

【００１１】

例えば、鍵を用いてプログラムを暗号化する手法があるが、複数のプログラムが存在した場合、解読が難しいようにプログラム毎に個別な鍵（例えば、擬似乱数の種など）を使用して、個別にプログラムを暗号化することが望ましい。しかしながら、個別に暗号化するために、有限な数の鍵を多く消費し、プログラム毎に鍵を変える処理が余分に必要となる課題があった。

【００１２】

また例えば、LZ（Lempel Ziv）法、適応的算術符号化法、または、動的ハフマン符号化のような、徐々に辞書を構築していくような圧縮技法を用いて個別にプログラムデータを圧縮する手法も考えられるが、プログラム毎に辞書を再構築する必要があり、まとめて圧縮するよりも圧縮率が悪くなる課題があった。

【００１３】

さらにまた例えば、同じインストラクションセットを使用しているプログラムにおいては、統計的な性質が似ており、特に、同じシステム上の同じリソースを使用するようなプログラムにおいては、アドレス情報や各種デバイスの設定値情報などのデータについても統計的な性質が似ている。この性質を利用して、プログラムをまとめて圧縮することにより、辞書が有効利用できることが望ましい。しかしながら、複数のプログラムをまとめて圧縮し、さらに、圧縮された複数のプログラムを暗号化するような手法は存在しなかった。

【００１４】

本発明はこのような状況に鑑みてなされたものであり、複数のプログラムをま

とめて圧縮し、かつ、圧縮された複数のプログラムを暗号化することにより、プログラムの記憶容量の削減、およびリバースエンジニアリングを防止することができるようにするものである。

【００１５】

【課題を解決するための手段】

本発明の第１の情報処理装置は、複数のデータを結合して圧縮する圧縮手段と、複数のデータに関する第１の付随データを生成する第１の生成手段と、圧縮手段により圧縮されたデータを、第１の生成手段により生成された第１の付随データとともに暗号化する暗号化手段とを備えることを特徴とする。

【００１６】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

【００１７】

前記第１の付随データは、複数のデータの個数および大きさに関するデータであるものとすることができる。

【００１８】

前記圧縮されたデータに関する第２の付随データを生成する第２の生成手段と、暗号化されたデータ、および、第２の生成手段により生成された第２の付随データを格納する格納手段とをさらに設けるようにすることができる。

【００１９】

前記第２の付随データは、圧縮されたデータの大きさに関するデータであるものとすることができる。

【００２０】

本発明の第１の情報処理方法は、複数のデータを結合して圧縮する圧縮ステップと、複数のデータに関する付随データを生成する生成ステップと、圧縮ステップの処理により圧縮されたデータを、生成ステップの処理により生成された付随データとともに暗号化する暗号化ステップとを含むことを特徴とする。

【００２１】

本発明の第１の情報処理装置および方法においては、複数のデータが結合されて圧縮され、複数のデータに関する付随データが生成され、圧縮されたデータが

付随データとともに暗号化される。

【００２２】

本発明の第２の情報処理装置は、暗号化されたデータを復号する復号手段と、復号手段により、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データを復元し、複数のデータが結合されて圧縮されたデータを伸張する伸張手段とを備えることを特徴とする。

【００２３】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

【００２４】

前記付随データは、複数のデータの個数および大きさに関するデータであるものとすることができる。

【００２５】

前記付随データに基づいて、複数のデータの所在に関する管理テーブルを作成する作成手段と、複数のデータ、および作成手段により作成された管理テーブルを記憶する記憶手段とをさらに設けるようにすることができる。

【００２６】

本発明の第２の情報処理方法は、暗号化されたデータを復号する復号ステップと、復号ステップの処理により、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データを復元し、複数のデータが結合されて圧縮されたデータを伸張する伸張ステップとを含むことを特徴とする。

【００２７】

本発明の第２の情報処理装置および方法においては、暗号化されたデータが復号されて、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データが復元され、複数のデータが結合されて圧縮されたデータが伸張される。

【００２８】

本発明の第３の情報処理装置は、複数のデータを結合して圧縮する圧縮手段と、複数のデータに関する第１の付随データを生成する第１の生成手段と、圧縮手段により圧縮されたデータを、第１の生成手段により生成された第１の付随デー

タとともに暗号化する暗号化手段と、圧縮されたデータに関する第２の付随データを生成する第２の生成手段と、暗号化されたデータ、および、第２の付随データを格納する格納手段と、格納手段に格納されている暗号化されたデータを復号する復号手段と、復号手段により、圧縮されたデータ、および、第１の付随データを復元し、圧縮されたデータを伸張する伸張手段と、伸張手段により伸張された複数のデータの中から、所定のデータを選択する選択手段と、選択手段により選択された所定のデータの処理を実行する実行手段とを備えることを特徴とする。

【００２９】

前記第２の付随データに基づいて、複数のデータの所在に関する管理テーブルを作成する作成手段と、伸張手段により伸張された複数のデータ、および作成手段により作成された管理テーブルを記憶する記憶手段とをさらに設けるようにすることができる。

【００３０】

前記実行手段には、記憶手段に記憶されている管理テーブルに基づいて、所定のデータの処理を実行させるようにすることができる。

【００３１】

前記復号手段による復号処理、および伸張手段による伸張処理の開始を指示するとともに、復号処理および伸張処理の終了を通知する通信手段をさらに設けるようにすることができる。

【００３２】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

【００３３】

前記第１の付随データは、複数のデータの個数および大きさに関するデータであり、第２の付随データは、圧縮されたデータの大きさに関するデータであるものとすることができる。

【００３４】

本発明の第３の情報処理方法は、複数のデータを結合して圧縮する圧縮ステップと、複数のデータに関する第１の付随データを生成する第１の生成ステップと

、圧縮ステップの処理により圧縮されたデータを、第１の生成ステップの処理により生成された第１の付随データとともに暗号化する暗号化ステップと、圧縮されたデータに関する第２の付随データを生成する第２の生成ステップと、暗号化されたデータ、および、第２の付随データを格納する格納ステップと、格納ステップの処理により格納された、暗号化されたデータを復号する復号ステップと、復号ステップの処理により、圧縮されたデータ、および、第１の付随データを復元し、圧縮されたデータを伸張する伸張ステップと、伸張ステップの処理により伸張された複数のデータの中から、所定のデータを選択する選択ステップと、選択ステップの処理により選択された所定のデータの処理を実行する実行ステップとを含むことを特徴とする。

【００３５】

本発明の第３の情報処理装置および方法においては、複数のデータが結合されて圧縮され、複数のデータに関する第１の付随データが生成され、圧縮されたデータとともに暗号化され、圧縮されたデータに関する第２の付随データが生成され、暗号化されたデータとともに格納される。また、暗号化されたデータが復号されて、圧縮されたデータ、および、第１の付随データが復元され、圧縮されたデータが伸張され、伸張された複数のデータの中から、所定のデータが選択され、処理が実行される。

【００３６】

【発明の実施の形態】

以下、図を参照して、本発明の実施の形態について説明する。

【００３７】

図１は、本発明を適用したマイクロコンピュータの構成例を示す図である。CPU（Central Processing Unit）１は、不揮発性メモリ２からRAM３に読み出された実行プログラムに従って各種の処理を実行する。

【００３８】

不揮発性メモリ２は、例えば、EEPROM（Electrically Erasable and Programmable Read Only Memory）やフラッシュメモリなどで構成され、圧縮および暗号化された、CPU１が各種の処理を実行する上において必要な実行プログラムなど

を記憶する。

【００３９】

RAM３は、例えば、DRAM（Dynamic Random Access Memory）やSRAM（Static RAM）などの読み書き可能なメモリで構成され、不揮発性メモリ２から読み出された実行プログラムを保存する他、その実行プログラムの開始アドレスなどを管理するプログラム管理テーブル５１（図３）も保存する。

【００４０】

CPU１、不揮発性メモリ２、およびRAM３は、バス４を介して相互に接続されている。

【００４１】

図２は、不揮発性メモリ２に格納されるデータの構造例を表わしている。同図に示されるように、予め決められた順番に実行プログラムＡ乃至Ｄが結合されたものがデータ２１とされ、不揮発性メモリ２に格納されている。

【００４２】

CPU１は、データ２１に含まれる実行プログラムの個数（図２の例の場合、４個）を表わす情報データ２２を生成するとともに、データ２１に含まれる各実行プログラムのサイズ（図２の例の場合、Ｓ１乃至Ｓ４）を表わす情報データ２３を生成する。

【００４３】

この情報データ２３により、複数の実行プログラムＡ乃至Ｄが結合されたデータ２１が不揮発性メモリ２からRAM３に読み出されても、CPU１は、データ２１内での相対的なアドレスを算出することができるため、各実行プログラムの開始アドレスを容易に知ることができる。

【００４４】

CPU１は、LZ77法などの慣用圧縮技法を用いて、複数の実行プログラムＡ乃至Ｄが結合されたデータ２１を圧縮し、プログラムデータ２４を生成するとともに、圧縮されたプログラムデータ２４のサイズ（図２の例の場合、Ｓ５）を表わす情報データ２５を生成する。

【００４５】

さらにCPU１は、圧縮されたプログラムデータ２４、情報データ（個数データ）２２、および情報データ（サイズデータ）２３の３つのデータを連結して１つのデータとして、それを擬似乱数と１方向性関数を使ったワンタイムパッド暗号などの慣用暗号化技法を用いて暗号化し、データ２６を生成する。ここで、プログラムデータ２４とデータ２６のデータサイズがほぼ同じになるように暗号化される。そして、暗号化されたデータ２６、および圧縮されたプログラムデータ２４のサイズを表わす情報データ２５が、不揮発性メモリ２に格納される。

【００４６】

図３は、不揮発性メモリ２に格納されている、暗号化されたデータ２６がCPU１により伸張され、実行プログラムとしてRAM３に保存され、実行されるまでの処理を模式的に示している。

【００４７】

なお、１つのCPUに対して複数のプログラムを対応させることができるものとするため、便宜上、CPU１を、CPU１－１乃至１－３として図示し、CPU１－１では実行プログラムＡが実行され、CPU１－２では、実行プログラムＢが実行され、CPU１－３では、実行プログラムＣまたは実行プログラムＤが実行されるものとする。

【００４８】

不揮発性メモリ２には、図２を用いて上述したように、暗号化されたデータ２６、および圧縮されたプログラムデータ２４のサイズを表わす情報データ２５が格納されている。

【００４９】

例えば、CPU１－１は、不揮発性メモリ２からデータ２６および情報データ２５を読み出し、暗号化されたデータ２６を復号して、プログラムデータ２４、情報データ２２、および情報データ２３を復元する。CPU１－１は、さらに、圧縮されたプログラムデータ２４を伸張してデータ２１を復元し、RAM３に保存する。ここで、CPU１－１は、情報データ２５により表わされているサイズ分のデータについて、全て復号処理および伸張処理したとき、それらの処理を終了した判断する。

【００５０】

復号処理および伸張処理において、ワンタイムパッド暗号とLZ77法のような逐次処理が可能な方法が組み合わされて用いられている場合には、CPU１－１は、プログラムデータ２４を保存するためのワークメモリを必要とせずに、復号処理および伸張処理を同時に行いつつ、データ２６からデータ２１へ直接変換することができる。

【００５１】

CPU１－１はまた、復元された情報データ２２および情報データ２３に基づいて、データ２１に含まれる実行プログラムの数とそれぞれのサイズを知ることができるため、それらの情報から各実行プログラムの先頭アドレスをそれぞれ算出し、各実行プログラムと、先頭アドレスおよびサイズの対応付けに関するプログラム管理テーブル５１を作成し、RAM３に保存する。

【００５２】

図３に示すプログラム管理テーブル５１においては、実行プログラムＡと、アドレス０１およびサイズ０１が対応付けられ、実行プログラムＢと、アドレス０２およびサイズ０２が対応付けられ、実行プログラムＣと、アドレス０３およびサイズ０３が対応付けられ、実行プログラムＤと、アドレス０４およびサイズ０４が対応付けられている。

【００５３】

このようにして、RAM３内において、プログラム管理テーブル５１により、データ２１に含まれる各実行プログラムＡ乃至Ｄが管理される。

【００５４】

例えば、予め決められたCPU１、または図示せぬ外部装置より指示されたCPU１（図３の例の場合、CPU１－１）は、RAM３に復元されたデータ２１、および、プログラム管理テーブル５１に基づいて、予め決められた実行プログラム、または、外部装置より指示された実行プログラムを実行可能な状態にして、それを実行する。

【００５５】

より具体的には、CPU１－１は、RAM３で管理されているプログラム管理テーブ

ル５１から、実行すべきプログラム（いまの場合、実行プログラムＡ）に対応付けられている先頭アドレス（いまの場合、アドレス０１）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出する。開始アドレスは、先頭アドレスからの相対アドレスが予め決められていれば、容易に算出することができる。そしてCPU１－１は、RAM３内における、算出された開始アドレスにジャンプし、実行プログラムＡの実行を開始する。

【００５６】

また、CPU１－２は、RAM３で管理されているプログラム管理テーブル５１から、実行すべきプログラム（いまの場合、実行プログラムＢ）に対応付けられている先頭アドレス（いまの場合、アドレス０２）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスにジャンプして、実行プログラムＢの実行を開始する。

【００５７】

同様に、CPU１－３も、RAM３で管理されているプログラム管理テーブル５１から、実行すべきプログラム（いまの場合、実行プログラムＣまたは実行プログラムＤ）に対応付けられている先頭アドレス（いまの場合、アドレス０３またはアドレス０４）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスにジャンプして、実行プログラムＣまたは実行プログラムＤの実行を開始する。

【００５８】

次に、図４のフローチャートを参照して、CPU１－１が実行する、複数のプログラムの格納処理について説明する。

【００５９】

ステップＳ１において、CPU１－１は、予め決められた順番、もしくは、図示せぬ外部装置より指示された順番に、複数の実行プログラムを結合する。これにより、図２で示したように、実行プログラムＡ乃至Ｄが結合されたデータ２１が生成される。

【００６０】

ステップＳ２において、CPU１－１は、ステップＳ１の処理で結合されたデー

タ２１に含まれる実行プログラムの個数を計数し、個数（図２の例の場合、４個）を表わすデータとして情報データ２２を生成する。ステップＳ３において、CPU１－１は、ステップＳ１の処理で結合されたデータ２１に含まれる各実行プログラムのサイズをそれぞれ算出し、サイズ（図２の例の場合、Ｓ１乃至Ｓ４）を表わすデータとして情報データ２３を生成する。

【００６１】

ステップＳ４において、CPU１－１は、ステップＳ１の処理で結合されたデータ２１を、LZ77法などの慣用圧縮技法を用いて圧縮し、プログラムデータ２４を生成する。ステップＳ５において、CPU１－１は、ステップＳ４の処理で圧縮されたプログラムデータ２４、ステップＳ２の処理で生成された情報データ（個数データ）２２、および、ステップＳ３の処理で生成された情報データ（サイズデータ）２３を連結し、それを擬似乱数と１方向性関数を使ったワンタイムパッド暗号などの慣用暗号化技法を用いて暗号化し、データ２６を生成する。

【００６２】

ステップＳ６において、CPU１－１は、ステップＳ４の処理で圧縮されたデータ２４のサイズを算出し、サイズ（図２の例の場合、Ｓ５）を表わすデータとして情報データ２５を生成する。ステップＳ７において、CPU１－１は、ステップＳ５の処理で暗号化されたデータ２６、および、ステップＳ６の処理で生成された情報データ（サイズデータ）２５を不揮発性メモリ２に格納する。

【００６３】

このように、複数の実行プログラムをまとめて圧縮することで、個別に圧縮する場合に較べてオーバヘッドが少なく、管理データの削減、および、伸張プログラムや伸張装置を簡素化することができる。

【００６４】

また、同一インストラクションセットを用いている実行プログラムは、統計的な性質が似ているため、個別に圧縮するよりも圧縮率の向上が期待できる。さらに、実行プログラムの個数に関する情報（情報データ２２）、および、実行プログラムの位置やサイズに関する情報（情報データ２３）を、複数の実行プログラムが結合され圧縮されたデータ（プログラムデータ２４）と一緒に暗号化するこ

とにより、その暗号化されたデータ（データ２６）から、実行プログラムに関する情報を推測するのが難しく、暗号解読をより困難にすることができる。

【００６５】

次に、図５のフローチャートを参照して、CPU１－１が実行する、不揮発性メモリ２に格納された複数のプログラムの伸張処理について説明する。

【００６６】

ステップＳ２１において、CPU１－１は、不揮発性メモリ２から、暗号化されたデータ２６、および情報データ（サイズデータ）２５を読み出す。ステップＳ２２において、CPU１－１は、ステップＳ２１の処理で読み出された、暗号化されたデータ２６をワンタイムパッド暗号などで復号し、圧縮されたプログラムデータ２４、情報データ（個数データ）２２、および情報データ（サイズデータ）２３を復元する。

【００６７】

ステップＳ２３において、CPU１－１は、ステップＳ２２の処理で復元された、圧縮されたプログラムデータ２４をLZ77法などで伸張し、実行プログラムＡ乃至Ｄが結合されたデータ２１を復元する。ステップＳ２４において、CPU１－１は、ステップＳ２２の処理で復元された情報データ（個数データ）２２および情報データ（サイズデータ）２３に基づいて、ステップＳ２３の処理で伸張されたデータ２１に含まれる各実行プログラムの先頭アドレスをそれぞれ算出し、各実行プログラムと、先頭アドレスおよびサイズの対応付けに関するプログラム管理テーブル５１を作成する。

【００６８】

ステップＳ２５において、CPU１－１は、ステップＳ２３の処理で復元された、実行プログラムＡ乃至Ｄが結合されたデータ２１、および、ステップＳ２４の処理で作成されたプログラム管理テーブル５１をRAM３に保存する。

【００６９】

このように、全ての実行プログラムの復号処理および伸張処理を連続して実行することができるため、処理の高速化および簡素化が期待できる。これにより、ソフトウェアでは、デコーダプログラムのサイズ削減につながり、ハードウェア

では、ゲート数の削減につながる。

【００７０】

また、上述したプログラム伸張処理により、RAM３には、複数の実行プログラムＡ乃至Ｄが結合されたデータ２１、および、各実行プログラムを管理するためのプログラム管理テーブル５１が保存されるため、CPU１は、迅速に、実行すべきプログラムのアドレスにジャンプして、そのプログラムの実行を開始することができる。

【００７１】

次に、図６のフローチャートを参照して、CPU１－１が実行する、RAM３に保存されたプログラムの実行処理について説明する。

【００７２】

ステップＳ４１において、CPU１－１は、所定のプログラム（例えば、実行プログラムＡ）の実行が指示されたか否かを判定し、所定のプログラムの実行が指示されるまで待機する。そして、ステップＳ４１において、所定のプログラムの実行が指示されたと判定された場合、ステップＳ４２に進み、CPU１－１は、RAM３に保存されているプログラム管理テーブル５１に基づいて、実行が指示された所定のプログラム（いまの場合、実行プログラムＡ）に対応付けられている先頭アドレス（いまの場合、アドレス０１）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出する。

【００７３】

ステップＳ４３において、CPU１－１は、RAM３内における、ステップＳ４２の処理で算出された開始アドレスにジャンプし、所定のプログラム（いまの場合、実行プログラムＡ）の実行を開始する。ステップＳ４４において、CPU１－１は、所定のプログラムの実行が終了したか否かを判定し、まだプログラム実行中であると判定した場合、ステップＳ４５に進む。

【００７４】

ステップＳ４５において、CPU１－１はさらに、図示せぬ外部装置より、実行中のプログラムの強制終了が指示されたか否かを判定し、強制終了が指示されていないと判定した場合、ステップＳ４４に戻り、上述した処理を繰り返し実行す

る。そして、ステップＳ４４において、所定のプログラムの実行が終了した、または、ステップＳ４５において、実行中のプログラムの強制終了が指示されたと判定された場合、処理は終了される。

【００７５】

このように、RAM３に、複数のプログラムが結合されて保存されていても、CPU１は、プログラム管理テーブル５１に基づいて、迅速に、実行すべきプログラムの開始アドレスにジャンプし、そのプログラムを実行することができる。

【００７６】

なお、上述した図４乃至図６の処理は、CPU１－１が実行する場合について説明したが、CPU１－２あるいはCPU１－３が実行することも勿論可能である。

【００７７】

以上においては、プログラム管理テーブル５１から、実行すべきプログラムに対応付けられている先頭アドレスを読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスへジャンプして、実行プログラムの実行を開始するようにしたが、例えば、図７に示されるように、実行すべきプログラムが格納されている場所を、CPU１が、プログラム管理テーブル５１の対応する実行プログラムの先頭アドレスから特定し、そのプログラムをプログラム実行可能な所定のメモリ領域６１に転送する。そして、実行すべきCPU１－１乃至１－３のいずれかが、メモリ領域６１内の所定アドレスへジャンプして、そのプログラムの実行を開始することもできる。ただし、この場合、メモリ領域６１と開始アドレスは予め決められているものとする。

【００７８】

このように、特定のメモリ領域６１として、LSI内にCPUと混載されたSRAMやDRAMなどを用いることで、高速なプログラム実行が可能となる。

【００７９】

また以上においては、CPU１－１が、暗号化されたデータ２６の復号処理、圧縮されたプログラムデータ２４の伸張処理、および、プログラム管理テーブルの作成処理を行うようにしたが、例えば、図８に示されるように、専用のハードウェアである復号伸張処理装置７１を新たに設け、そこで、これらの処理を行わせ

るようにしてもよい。

【００８０】

この場合、図示せぬ外部装置から、または、CPU１－１乃至１－３から通信手段７２を介して、復号伸張処理装置７１に対して、復号処理および伸張処理の実行を指示することにより開始される。ここで、通信手段７２としては、専用の信号やバス上のレジスタなどで実現することができる。

【００８１】

この指示を受けた復号伸張処理装置７１は、図５を用いて上述したような復号処理および伸張処理を実行する。すなわち、復号伸張処理装置７１は、不揮発性メモリ２から、暗号化されたデータ２６、および情報データ２５を読み出し（ステップＳ２１）、暗号化されたデータ２６を復号して圧縮されたプログラムデータ２４、情報データ２２、および情報データ２３を復元し（ステップＳ２２）、圧縮されたプログラムデータ２４を伸張して実行プログラムＡ乃至Ｄが結合されたデータ２１を復元し（ステップＳ２３）、情報データ２２および情報データ２３に基づいて、プログラム管理テーブル５１を作成し（ステップＳ２４）、RAM３に保存する（ステップＳ２５）。

【００８２】

そして復号伸張処理装置７１は、処理が完了した旨を、通信手段７２を介してCPU１に通知する。このように、CPU１は、通信手段７２により、復号伸張処理装置７１の処理内容を知ることができる。また通信手段７２を利用することで、例えば、CPU１のリセットが解除されること、復号伸張処理装置７１がCPU１へ割り込みを発行すること、または、復号伸張処理装置７１のステータスレジスタをCPU１がポーリングすることなどの実装も可能となる。

【００８３】

以上のようにしてRAM３に復元されたデータ２１およびプログラム管理テーブル５１を用いて、CPU１－１乃至１－３は、図示せぬ外部装置からの指示により、または、予め決められたようにして、所定の実行プログラムを実行することができる。ここで、「予め決められたようにして」とは、先に実行されたプログラムの中に、次にどのプログラムをどのようにして実行すべきかが記述されている

場合を含むものとする。

【００８４】

以上においては、LSI内にCPU１と混載されたSRAMやDRAMなどを用いるようにしたが、LSI内部のSRAMについては、CPU１が高速アクセスすることが可能であるが、大容量を搭載することが難しい。そこで、例えば、LSI内部ほど高速アクセスが可能ではないが、大容量であるLSI外部のDRAMにデータ２１を格納しておき、CPU１が所定のプログラムを実行する場合に、そのプログラムをLSI外部のDRAMからLSI内部のSRAMへコピーしてから実行を開始するようなシステムも考えられる。

【００８５】

このようなシステムでは、特定のメモリ領域に内部SRAMを割り当て、状況に応じて複数のプログラムを入れ替えることで、より多くの機能を高速にLSI内部のSRAMで実行することができる。

【００８６】

以上のように、CPUの数以上の実行プログラムをデータ２１に含むことは多分にあり、実行プログラムの数を、LSI内部のCPUの数からは推測することができない。従って、複数の実行プログラムがまとめて圧縮され、さらに暗号化されているデータ２６は、その暗号化および圧縮率が隠蔽され、より強固にリバースエンジニアリングを防止することができる。

【００８７】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。

【００８８】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００８９】

【発明の効果】

以上のように、第１の本発明によれば、データの記憶容量を削減することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの記憶容量を削減するとともに、リバースエンジニアリングを防止することが可能となる。

【００９０】

第２の本発明によれば、データ処理の高速化および簡素化を実現することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの復号伸張処理の高速化および簡素化を実現することが可能となる。

【００９１】

第３の本発明によれば、データの記憶容量を削減し、データ処理の高速化および簡素化を実現することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの記憶容量を削減するとともに、圧縮および暗号化された複数の実行プログラムの復号伸張処理の高速化および簡素化を実現することが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用したマイクロコンピュータの構成例を示す図である。

【図２】

ROMに格納されるデータの構造例を表わす図である。

【図３】

暗号化されたデータが伸張され実行されるまでの処理を模式的に示す図である。

【図４】

複数のプログラムの格納処理を説明するフローチャートである。

【図５】

複数のプログラムの伸張処理を説明するフローチャートである。

【図６】

プログラムの実行処理を説明するフローチャートである。

【図７】

暗号化されたデータが伸張され実行されるまでの他の処理を模式的に示す図で

ある。

【図８】

暗号化されたデータが伸張され実行されるまでの他の処理を模式的に示す図である。

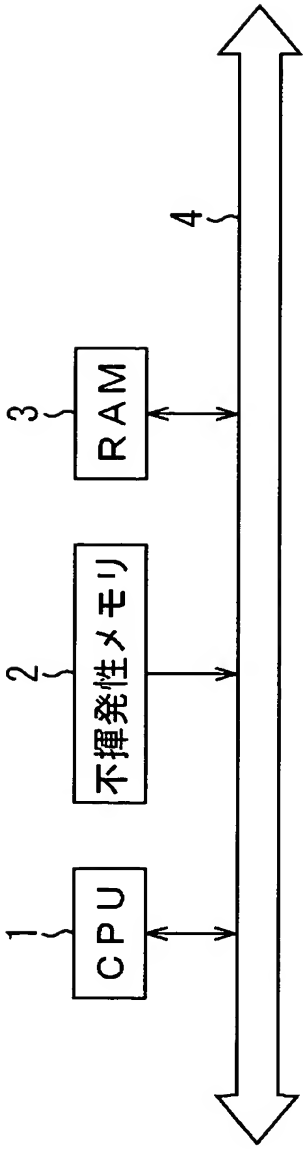
【符号の説明】

１　CPU,　２　不揮発性メモリ,　３　RAM,　７１　復号伸張装置

【書類名】図面

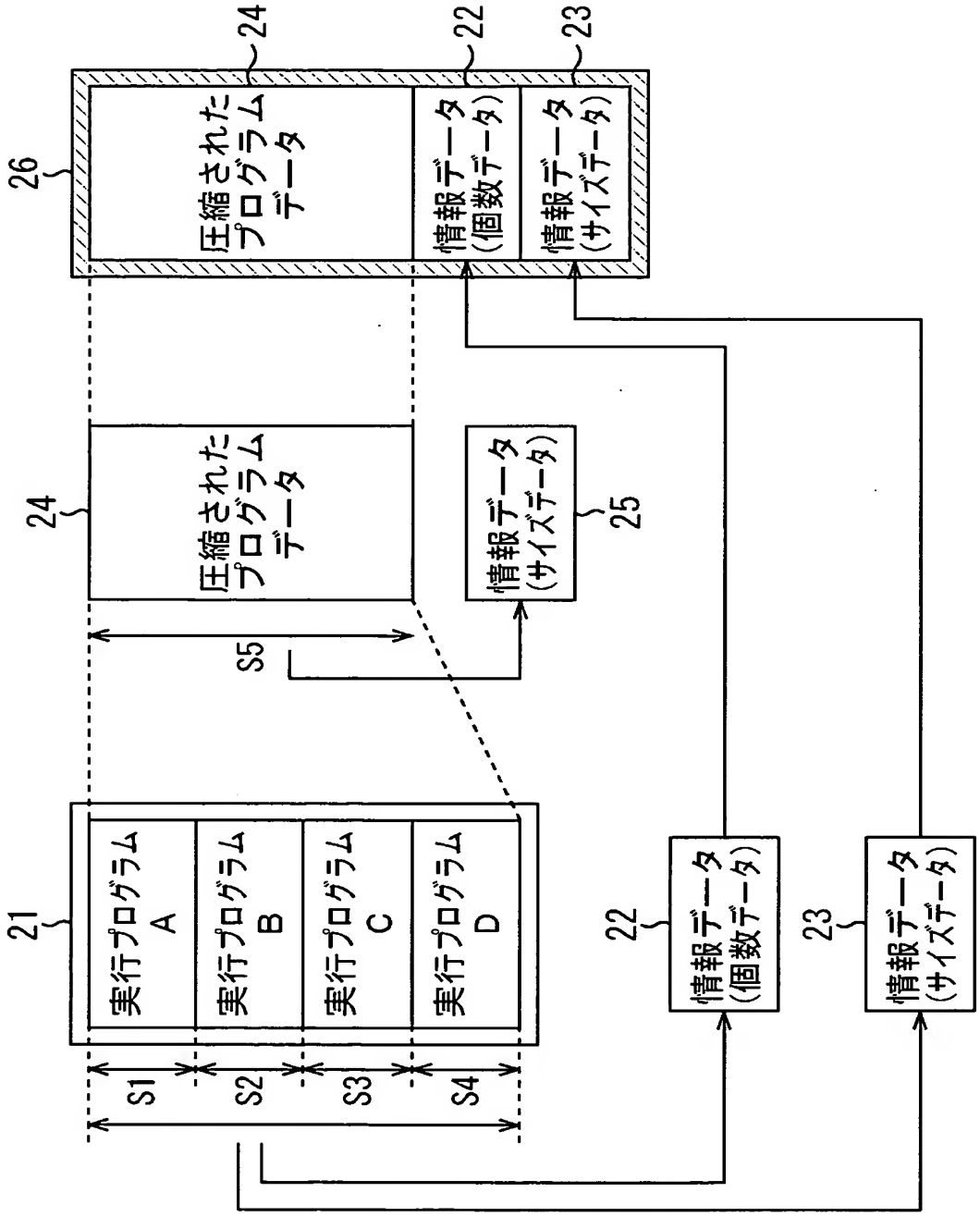
【図１】

図1



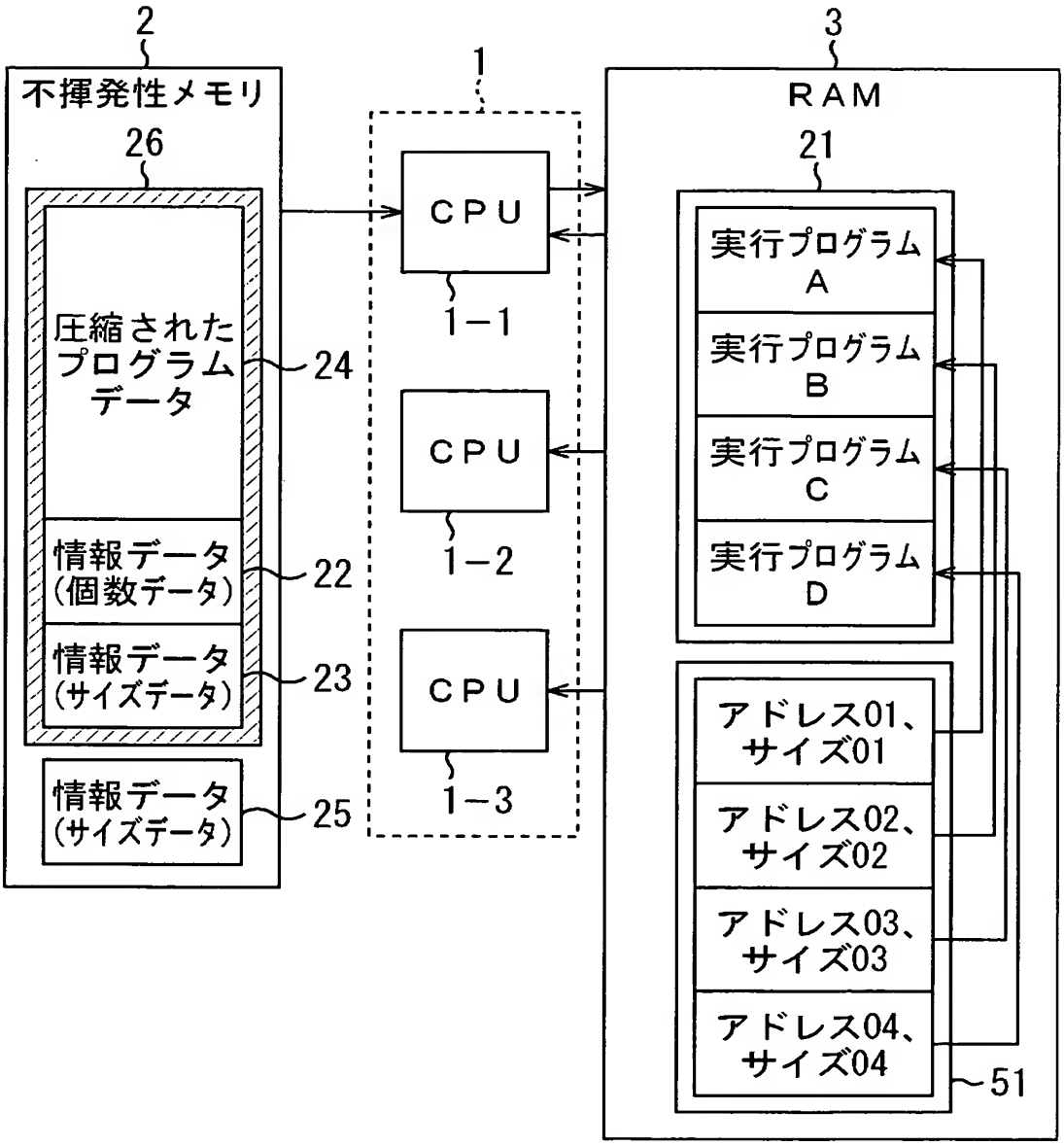
【図２】

図2


24
22
23
26
圧縮されたプログラムデータ
情報データ（個数データ）
情報データ（サイズデータ）
24
圧縮されたプログラムデータ
情報データ（サイズデータ）
25
S5
21
実行プログラムA
実行プログラムB
実行プログラムC
実行プログラムD
22
情報データ（個数データ）
23
情報データ（サイズデータ）
S1
S2
S3
S4

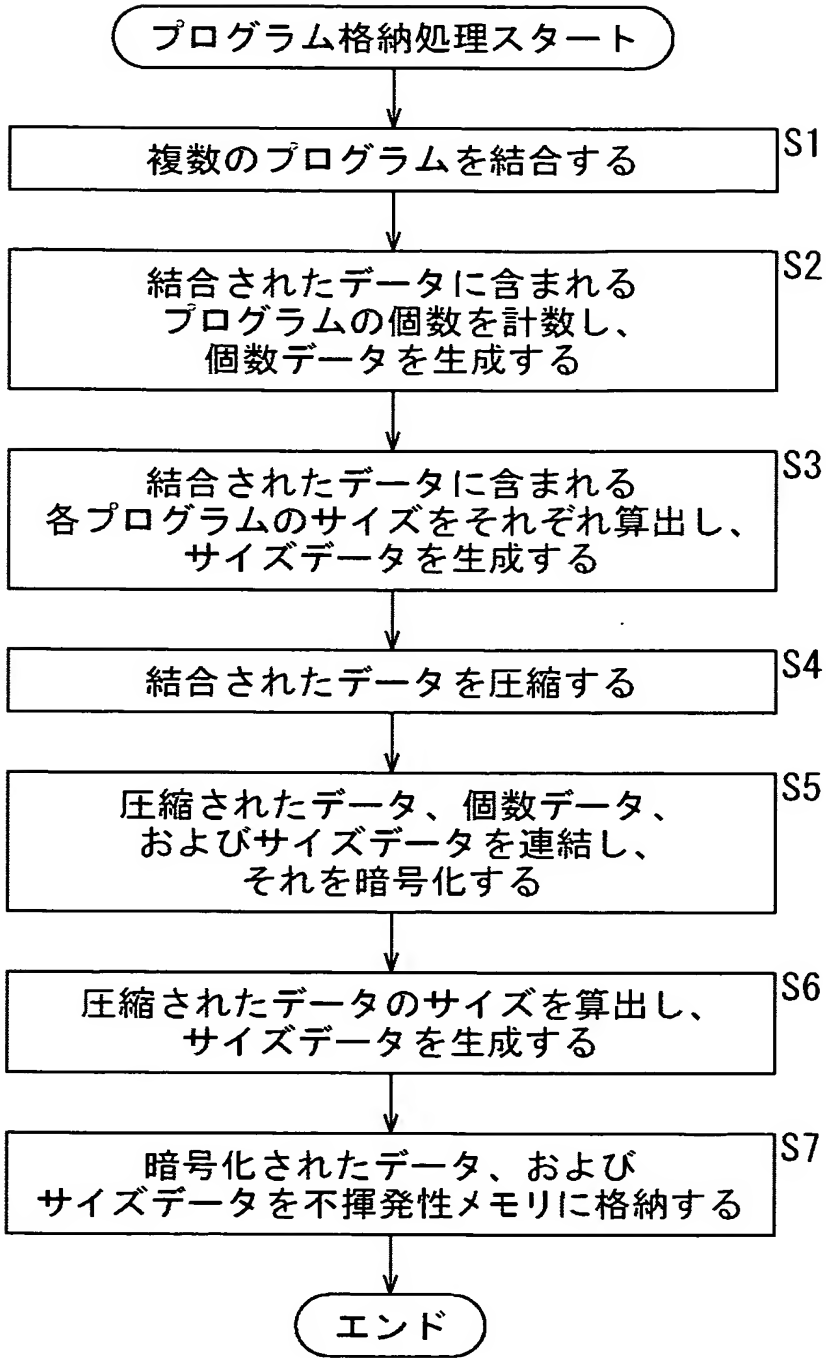
【図３】

図3


2
不揮発性メモリ
26
圧縮されたプログラムデータ
24
情報データ(個数データ)
22
情報データ(サイズデータ)
23
情報データ(サイズデータ)
25
1
CPU
1−1
CPU
1−2
CPU
1−3
3
RAM
21
実行プログラムA
実行プログラムB
実行プログラムC
実行プログラムD
アドレス01、サイズ01
アドレス02、サイズ02
アドレス03、サイズ03
アドレス04、サイズ04
51

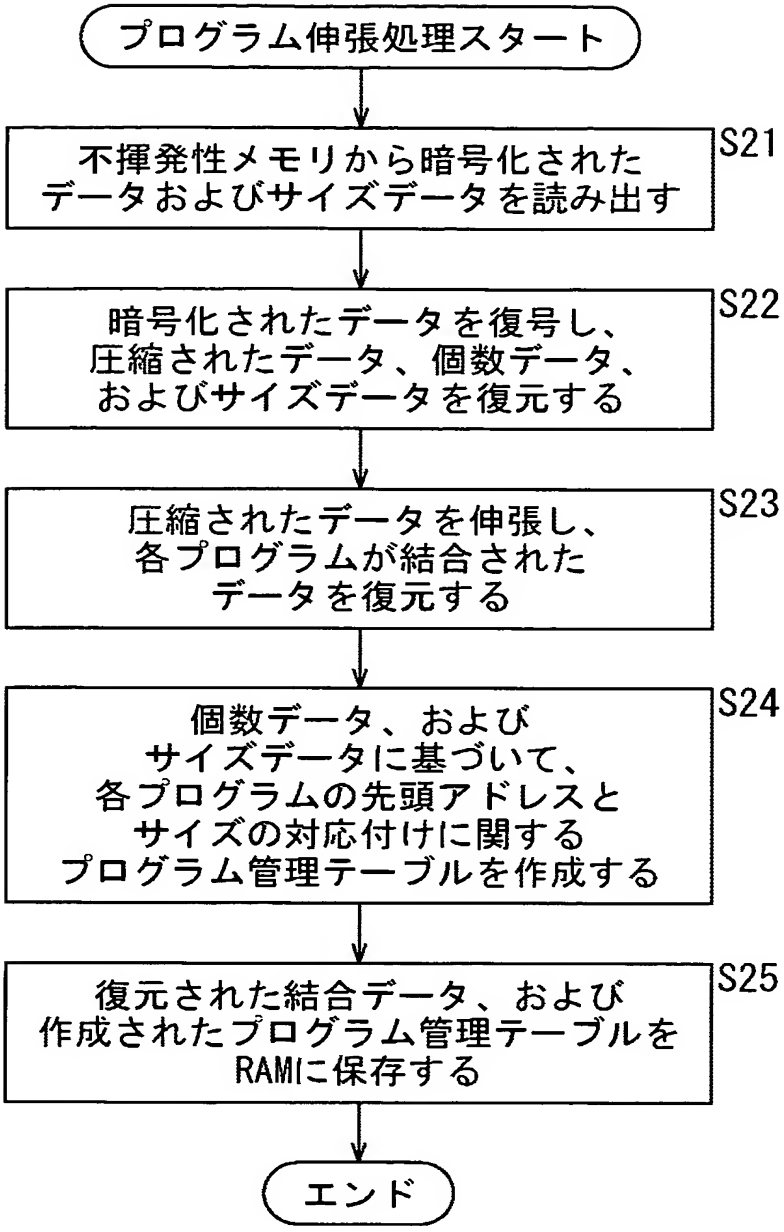
【図４】

図4


プログラム格納処理スタート
複数のプログラムを結合する
S1
結合されたデータに含まれる
プログラムの個数を計数し、
個数データを生成する
S2
結合されたデータに含まれる
各プログラムのサイズをそれぞれ算出し、
サイズデータを生成する
S3
結合されたデータを圧縮する
S4
圧縮されたデータ、個数データ、
およびサイズデータを連結し、
それを暗号化する
S5
圧縮されたデータのサイズを算出し、
サイズデータを生成する
S6
暗号化されたデータ、および
サイズデータを不揮発性メモリに格納する
S7
エンド

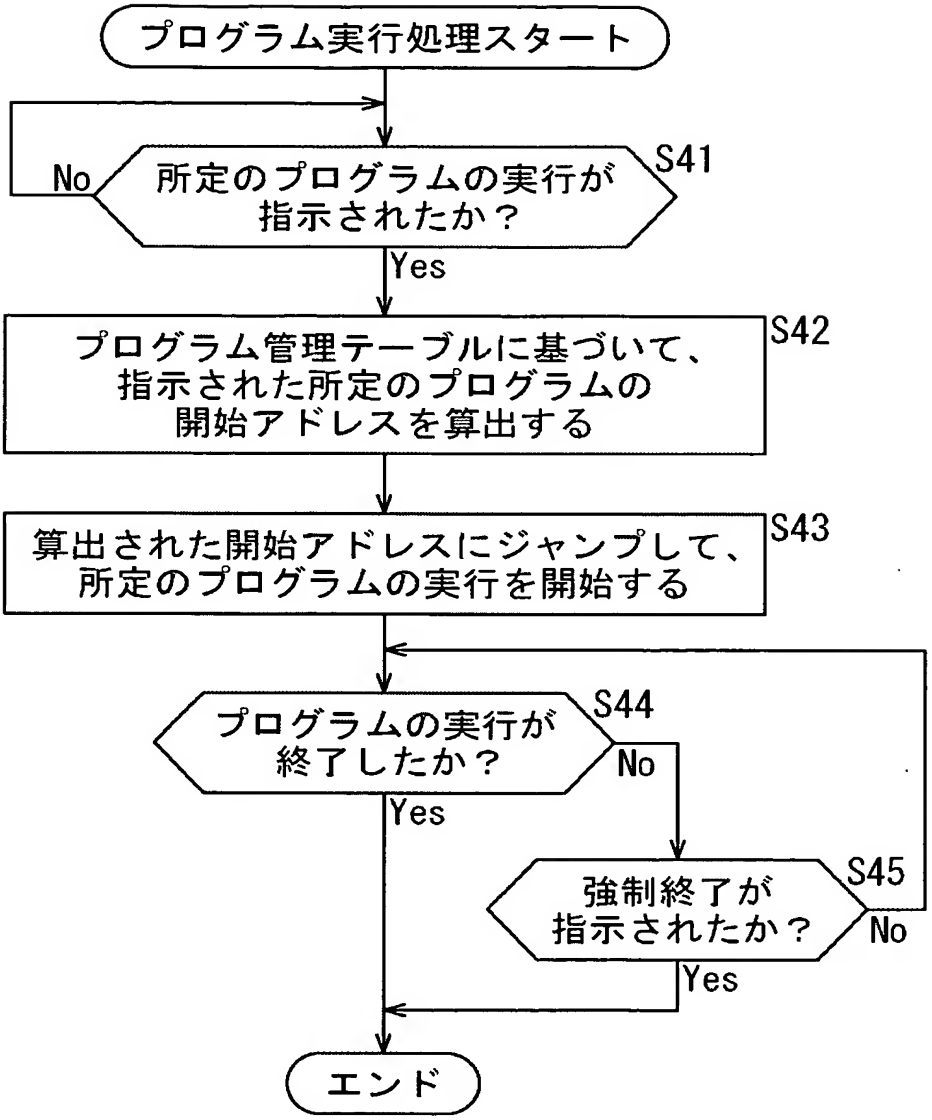
【図５】

図5


プログラム伸張処理スタート
不揮発性メモリから暗号化された
データおよびサイズデータを読み出す
S21
暗号化されたデータを復号し、
圧縮されたデータ、個数データ、
およびサイズデータを復元する
S22
圧縮されたデータを伸張し、
各プログラムが結合された
データを復元する
S23
個数データ、および
サイズデータに基づいて、
各プログラムの先頭アドレスと
サイズの対応付けに関する
プログラム管理テーブルを作成する
S24
復元された結合データ、および
作成されたプログラム管理テーブルを
RAMに保存する
S25
エンド

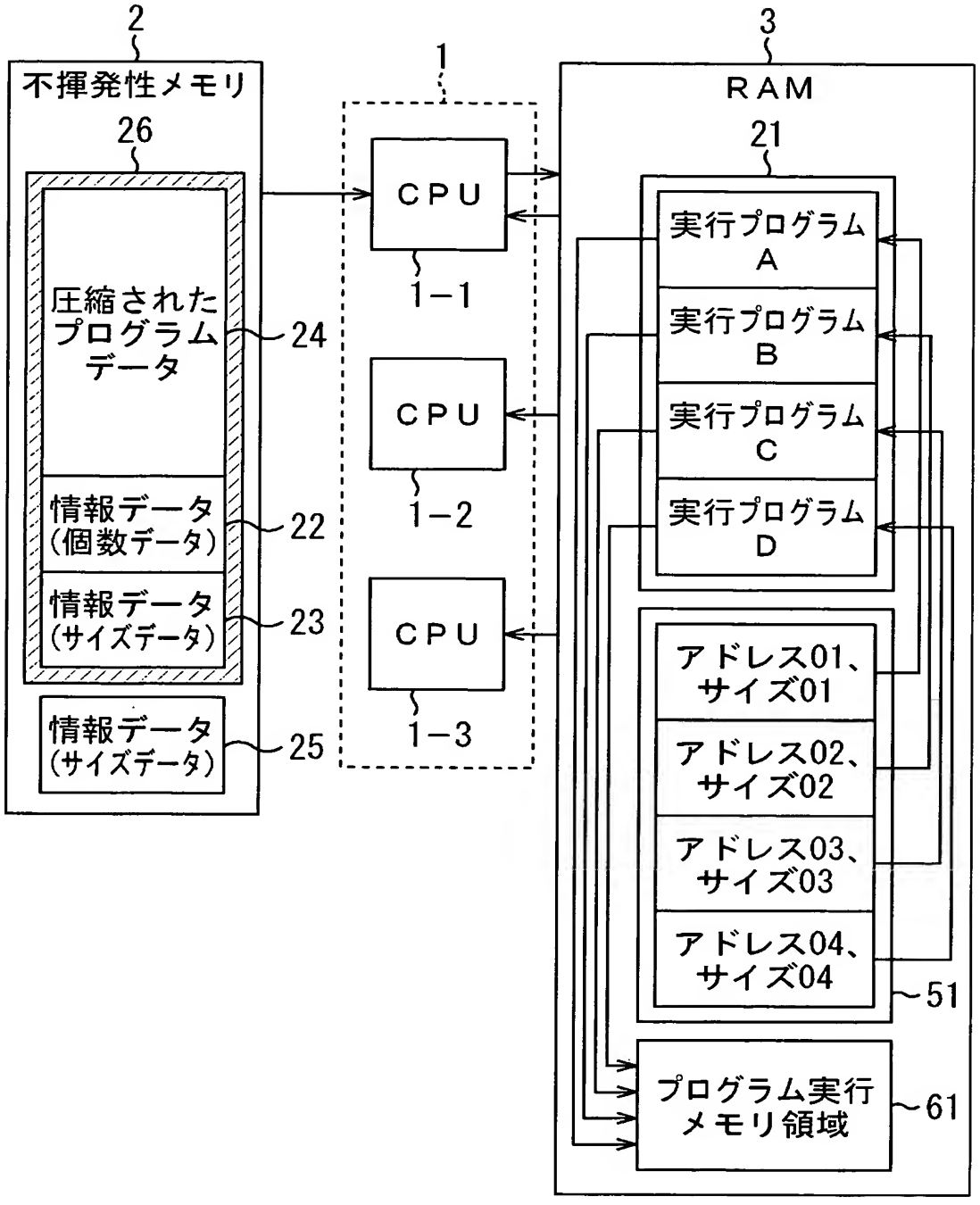
【図６】

図6


プログラム実行処理スタート
No
所定のプログラムの実行が
指示されたか？
S41
Yes
プログラム管理テーブルに基づいて、
指示された所定のプログラムの
開始アドレスを算出する
S42
算出された開始アドレスにジャンプして、
所定のプログラムの実行を開始する
S43
プログラムの実行が
終了したか？
S44
No
Yes
強制終了が
指示されたか？
S45
No
Yes
エンド

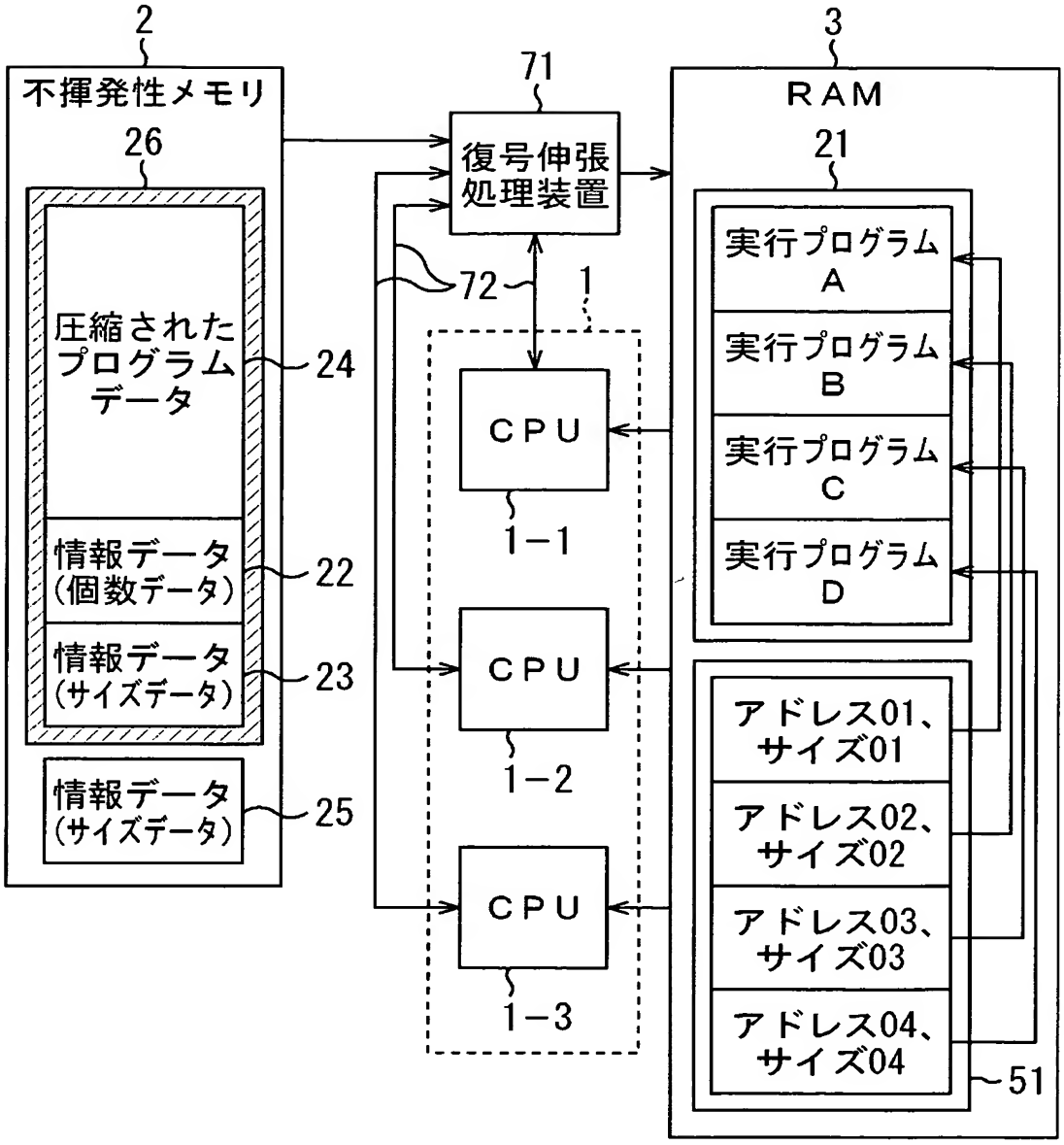
【図７】

図7


2
不揮発性メモリ
26
圧縮されたプログラムデータ
24
情報データ(個数データ)
22
情報データ(サイズデータ)
23
情報データ(サイズデータ)
25
1
CPU
1−1
CPU
1−2
CPU
1−3
3
RAM
21
実行プログラムA
実行プログラムB
実行プログラムC
実行プログラムD
アドレス01、サイズ01
アドレス02、サイズ02
アドレス03、サイズ03
アドレス04、サイズ04
51
プログラム実行メモリ領域
61

【図８】

図8


2
不揮発性メモリ
26
圧縮されたプログラムデータ
24
情報データ(個数データ)
22
情報データ(サイズデータ)
23
情報データ(サイズデータ)
25
71
復号伸張処理装置
72
1
CPU
1−1
CPU
1−2
CPU
1−3
3
RAM
21
実行プログラムA
実行プログラムB
実行プログラムC
実行プログラムD
アドレス01、サイズ01
アドレス02、サイズ02
アドレス03、サイズ03
アドレス04、サイズ04
51

【書類名】　　要約書

【要約】

【課題】　プログラムの記憶容量の削減、およびリバースエンジニアリングを防止することができるようにする。

【解決手段】　不揮発性メモリ２には、データ２１が圧縮されたプログラムデータ２４、データ２１に含まれる実行プログラムの個数を表わす情報データ２２、および各実行プログラムのサイズを表わす情報データ２３が連結されて暗号化されたデータ２６が格納されている。CPU１－１は、不揮発性メモリ２からデータ２６を読み出して復号し、プログラムデータ２４、および情報データ２２，２３を復元した後、プログラムデータ２４を伸張してデータ２１を復元し、RAM３に保存する。CPU１－１はまた、情報データ２２，２３に基づいて、各実行プログラムを管理するためのプログラム管理テーブル５１を作成し、RAM３に保存する。本発明は、マイクロコンピュータに適用できる。

【選択図】　　図３

特願２００２－３７２５２１

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社